UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,718	03/18/2004	Kevin Eugene Dombkowski	LUC-469/Dombkowski 11-16	6988

32205 7590 09/24/2009

Carmen Patti Law Group , LLC
ONE N. LASALLE STREET
44TH FLOOR
CHICAGO, IL 60602

EXAMINER	
YALEW, FIKREMARIAM A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
09/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/803,718	DOMBKOWSKI ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the applicant arguments filed on 07/24/2009, **PROSECUTION IS HEREBY REOPENED**.A new art rejection has been applied as set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

2. Claims 1-27 are pending.

3. Examiner withdraws 35 USC 112 rejection based on the applicant argument.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6, 8-18, 20-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karaoguz (US Pub No 2004/0059914 A1) in view of Epstein et al(hereinafter referred as Epstein) US Patent No 5,517,567.

6. As per claim 1: Karaoguz discloses an apparatus/method/article, comprising: an authentication device that authenticates a computing device (See 0041, 0049(i.e., **receive a request message on the first wireless device and the wireless device can operate as an authentication device**)), in communication with the authentication device, through employment of a determination that a current location of the authentication device matches an initial location of the authentication device (See Fig 3 steps 305,310 and 0019,0022,0039(i.e. **determining the location of information of the user and identify the user based on the location of the information**).

Karaoguz does not explicitly teach wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device.

However Epstein teaches wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device (See col.6 lines 52 through col.7 line 6(i.e., **any attempts to remove remote unit from its installed location with cut off external power supply and will result in the immediate loss of all memory including SN1 and SN2**))

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Mackenzie within

Karaoguz method in order to securely distributing a communication key from a master unit to a remote unit.

7. As per claim 2: the combinations of Karaoguz-Epstein teach the apparatus wherein the computing device comprises a first computing device wherein the authentication device makes the determination that the current location of the authentication device matches the initial location of the authentication device in response to a request from a second computing device for authentication of the first computing device for a data transfer from the second computing device to the first computing device (See Karaoguz 0008,0019-0020).

8. As per claim 3: the combinations of Karaoguz-Epstein teach the apparatus wherein the request from the second computing device comprises an authentication challenge string (See Karaoguz 0038,0041); wherein the authentication device stores one or more private keys, wherein if the current location of the authentication device matches the initial location of the authentication device, then the authentication device employs one or more of the one or more private keys to decrypt the authentication challenge string into an authentication challenge response(See Karaoguz 0038).

9. As per claim 4: the combinations of Karaoguz-Epstein teach the apparatus wherein the authentication device sends the authentication challenge response to the second computing device, wherein the second computing device analyzes the authentication challenge response to determine whether the first computing device is authenticated for the data transfer (See Karaoguz 0037-0038).

10. As per claim 5: the combinations of Karaoguz-Epstein teach the apparatus wherein the second computing device comprises an authentication challenge key to

compare with the authentication challenge response received from the authentication device (See Karaoguz 0038,0041); wherein if the authentication challenge response matches the authentication challenge key, then the authentication challenge response represents that the first computing device is authenticated and the data transfer can be sent from the second computing device to the first computing device(See Karaoguz Fig 4 step 440 and 0038,0041).

11. As per claim 6: the combinations of Karaoguz-Epstein teach the apparatus wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device prevents authentication of the first computing device and disables the one or more private keys (See Epsteincol.6 lines 52 through col.7 line 6).

12. As per claim 8: the combinations of Karaoguz-Epstein teach the apparatus wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the computing device; wherein the base portion is fixed to a surface near the computing device, wherein the cover portion is fixed to the base portion to provide a secure shell for the one or more electronic components (See Karaoguz Figs 2, 3 and 0017, 0050).

13. As per claim 9: the combinations of Karaoguz-Epstein teach the apparatus wherein a first one of the base and cover portions receives electricity through a power port, wherein a second one of the base and cover portions receives electricity through an electrical contact with the first one of the base and cover portions(See Karaoguz Fig 5 step 515,525); wherein upon separation of the second one of the base and cover portions from the first one of the base and cover portions, the second one of the base and cover

portions loses power and prevents authentication of the computing device(See Karaoguz Fig 5 step 515,525).

14. As per claim 10: the combinations of Karaoguz-Epstein teach wherein the second one of the base and cover portions electrically supports one or more of the one or more electronic components that store one or more private keys, wherein the authentication device employs one or more of the one or more private keys to authenticate the computing device (See Karaoguz Fig 5 step 515,525); wherein a loss of power in the second one of the base and cover portions erases the one or more private keys from the one or more of the one or more electronic components(See Epsteincol.6 lines 52 through col.7 line 6).

15. As per claim 11: the combinations of Karaoguz-Epstein teach the apparatus wherein the authentication device comprises a location sensor (See 0039); wherein upon initialization of the authentication device, the location sensor sets the initial location of the authentication device (See Karaoguz 0039,0045); wherein the location sensor determines the current location of the authentication device, wherein the authentication device compares the current location with the initial location to authenticate the computing device (See Karaoguz 0039,0045).

16. As per claim 12: the combinations of Karaoguz-Epstein teach the apparatus wherein the location sensor comprises a global positioning system component, wherein the global positioning system component measures the initial location and the current location of the authentication device as a three-dimensional location of latitude, longitude, and altitude (See Karaoguz 0045-0046).

17. As per claim 13: the combinations of Karaoguz-Epstein teach the apparatus

wherein the authentication device allows authentication of the computing device upon the determination that the authentication device matches the initial location of the authentication device within a specified error message (See Karaoguz 0039, 0045)

18. As per claims 14, 22: Karaoguz discloses an apparatus comprising: receiving a request from a second computing device to authenticate a first computing device for the data transfer from the second device to the first computing device(See 0041,0049(i.e., **receive a request message on the first warless device and the wireless device can operate as an authentication device**)) ;determining a current location of an authentication device, in response to the request from the second computing device(See Fig 3 steps 305,310 and 0019,0022(i.e. **determining the location of information of the user and identify the user based on the location of the information**)); and authenticating the first computing device if the current location of the authentication device matches an initial location of the authentication an authentication device that authenticates a computing device (See 0022,0039(i.e., **using signal generated location information to identify and authenticate available device**))

Karaoguz does not explicitly teach wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device. However Epstein teaches wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device (See col.6 lines 52 through col.6 line 6(i.e., **any attempts to remove remote unit from its installed location with cut off external power supply and will result in the immediate loss of all memory including SN1 and SN2**))

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Mackenzie within Karaoguz method in order to securely distributing a communication key from a master unit to a remote unit.

19. As per claim 15: the combinations of Karaoguz-Epstein teach the method wherein the request from the second computing device comprises an authentication challenge string (See Karaoguz 0038,0041); wherein the authentication device stores one or more private keys, wherein if the current location of the authentication device matches the initial location of the authentication device, then the authentication device employs one or more of the one or more private keys to decrypt the authentication challenge string into an authentication challenge response(See Karaoguz 0038).

20. As per claim 16: the combinations of Karaoguz-Epstein teach the method wherein the authentication device sends the authentication challenge response to the second computing device, wherein the second computing device analyzes the authentication challenge response to determine whether the first computing device is authenticated for the data transfer (See Karaoguz 0037-0038).

21. As per claim 17: the combinations of Karaoguz-Epstein teach the method wherein the second computing device comprises an authentication challenge key to compare with the authentication challenge response received from the authentication device (See Karaoguz 0038,0041); wherein if the authentication challenge response matches the authentication challenge key, then the authentication challenge response represents that the first computing device is authenticated and the data transfer can be sent from the

second computing device to the first computing device(See Karaoguz Fig 4 step 440 and 0038,0041).

22. As per claim 18: the combinations of Karaoguz-Epstein teach the method wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device prevents authentication of the first computing device and disables the one or more private keys (See Epsteincol.6 lines 52 through col.7 line 6).

23. As per claim 20: the combinations of Karaoguz-Epstein teach the method wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the computing device; wherein the base portion is fixed to a surface near the computing device, wherein the cover portion is fixed to the base portion to provide a secure shell for the one or more electronic components (See Karaoguz Figs 2, 3 and 0017, 0050).

24. As per claim 21: the combinations of Karaoguz-Epstein teach the method wherein a first one of the base and cover portions receives electricity through a power port, wherein a second one of the base and cover portions receives electricity through an electrical contact with the first one of the base and cover portions(See Fig 5 step 515,525); wherein upon separation of the second one of the base and cover portions from the first one of the base and cover portions, the second one of the base and cover portions loses power and prevents authentication of the computing device(See Karaoguz Fig 5 step 515,525).

25. As per claim 23: the combination of Karaoguz-Epstein teach the apparatus wherein the one or more private keys are erased upon an attempt of open the authentication device (See Epstein col.6 lines 52 through col.6 line 6)

26. As per claim 24: the combination of Karaoguz-Epstein teach the apparatus wherein the one or more private keys are erased via an automatic cutoff of power upon the attempt to move the authentication device (See Epstein col.6 lines 52 through col.6 line 6).

27. As per claim 25: the combination of Karaoguz-Epstein teach the appratus wherein the one or more private keys are erased via an automatic cutoff of power upon an attempt to open the authentication device (See Epstein col.6 lines 52 through col.6 line 6)

28. As per claim 26: the combination of Karaoguz-Epstein teach the apparatus wherein the current location comprises a network (See Karaoguz 0009 and Fig 2 step 205).

29. As per claim 27: the combination of Karaoguz-Epstein teach the apparatus wherein the current location comprises a room (See Epstein col.6 lines 52 through col.6 line 6).

30. **Claims 7, 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Karaoguz (US Pub No 2004/0059914 A1) in view of Epstein et al(hereinafter referred as Epstein) US Patent No 5,517,567 and further in view of Kobayshi et al(hereinafter referred as Kobayshi) JP 2003323599.**

31. As per claims 7, 19: the combination of Karaoguz-Epstein teach claims 6 and 15 as recited above. Karaoguz-Epstein do not explicitly teach the apparatus wherein the authentication device stores the one or more private keys in volatile memory, wherein

upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys.

However Kobayashi the apparatus wherein the authentication device stores the one or more private keys in volatile memory, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys(See 0005,0011).

Therefore it would have been obvious to one ordinary skill in art at that time the invention was made to modify the teaching method of Kobayashi within Epstein method in order to enhance security of the system.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

09/17/2009
/Fikremariam Yalew/
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436